



Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)

Approved for use through xx/xx/200x. OMB 0651-00xx  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional)	
		35997-215058	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]  on _____  Signature _____  Typed or printed name _____		Application Number	Filed
		09/919,958	August 2, 2001
		First Named Inventor	
		Bruno COUILLARD	
		Art Unit	Examiner
		2137	Michael J. Pyzocha
Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.			
This request is being filed with a notice of appeal.			
The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.			
I am the			
<input type="checkbox"/> applicant/inventor.		<u>Edward W. Yee</u> Signature	
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)		Edward W. Yee Typed or printed name	
<input checked="" type="checkbox"/> attorney or agent of record. Registration number <u>47,294</u>		202-344-4632 Telephone number	
<input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____		<u>Nov. 28, 2005</u> Date	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.			

<input checked="" type="checkbox"/> *Total of <u>1</u> forms are submitted.
---

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Bruno COUILLARD

Art Unit: 2137

Application No.: 09/919,958

Docket No.: 35997-215058

Conf. No. 4261

Examiner: Michael J. PYZOGA

Filed: August 2, 2001

For: METHOD AND SYSTEM FOR SECURELY  
TIMESTAMPING DIGITAL DATA

Customer No:

26694

PATENT TRADEMARK OFFICE

**PRE-APPEAL BRIEF REQUEST FOR REVIEW**

**MAIL STOP AF**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Dear Sir:

**Introductory Comments**

In response to the Advisory Office Action dated November 10, 2005, Applicant submits the following.

Applicant hereby authorizes the Office to charge the appeal fee and the one-month extension of time fee to Deposit Account No. 22-0261. No additional fees are believed to be required. However, if the Office deems that any additional fees are necessary, authorization is hereby granted to charge any additional required fees to Deposit Account No. 22-0261.

**Remarks**

Reconsideration of this Application is respectfully requested. In response to the Final Office Action mailed July 29, 2005 and the Advisory Action of November 10, 2005, Applicant submits the following. Claims 1-6, 8-18, and 20-25 are pending.

Based on the following remarks, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding objections and rejections.

**Response to Advisory Action**

On page 2, the Advisory Action responds to the remarks presented in the Request for Reconsideration filed October 28, 2005. The Advisory Action presents arguments in support of the rejection of claims 1-6, 8-18, and 20-25 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,001,752 to Fischer (hereinafter "Fischer"), in view of U.S. Patent No. 6,466,048 to Goodman (hereinafter "Goodman"), in further view of the Handbook of Applied Cryptography by Menezes et al. (hereinafter "Menezes"). The Advisory Action states that "Goodman is merely relied upon for its teaching of multiple modes," and that "when combined with Fischer the only keys available are those stored in the secret private key store (8) of figure 1, so these keys are used in the test mode of Goodman." The Advisory Action further states that column 7, lines 15-28 of Goodman teaches a test mode using an encryption processor 33. Applicant respectfully disagrees that the combination of Fischer and Goodman teach the features as recited in the claimed invention.

For at least the following reasons, Applicant disagrees with the above assertions made in the Advisory Action alleging that the cited references in combination render claim 1 obvious under 35 U.S.C. § 103(a).

The combined teachings of Fischer and Goodman do not teach providing an encryption processor that uses a single secure encryption key to perform different operations in multiple modes, in contrast with the statements made by the Final and Advisory Actions. Specifically, Goodman does not teach or suggest "the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations," as recited in claim 1. The following discusses the teachings of Fischer and Goodman as they relate to claim 1.

In FIG. 1, Fischer discloses a processor module 6 coupled to a storage device 8. The storage device stores a secret private key of a public/private key pair (also see Fischer, col. 4, lines 35-38). However, Fischer does not teach using the secret private key in multiple modes. Fischer also does not teach the processor module 6 using the secret private key in a first mode for encryption operations and for test operations and in a second mode in which the secret private key is only used for timestamping operations.

The Actions rely on Goodman for a teaching of these features. In its analysis, the Advisory Action states that Goodman is “merely relied upon for its teaching of multiple modes,” however, Fischer lacks more than a teaching of multiple modes. Fischer also lacks a teaching of the processor module 6 respectively performing the claimed encryption, test, and timestamping operations in the multiple modes using a single key.

However, Goodman does not provide such a teaching of an encryption processor performing the claimed operations in different modes using a single key. Instead, Goodman teaches an encryption processor useable in two modes, the test mode using a private test key, and the work mode using a separate secure electronic key (see Goodman, col. 5, lines 14-20, col. 5, lines 62-col. 6, line 2, col. 6, lines 55-56, also see col. 7, lines 15-28). Goodman also teaches a pseudo test mode that is not a true test mode (see Goodman, col. 8, lines 53-67). Goodman further teaches that once the test mode has been entered, test data, including the private test key, is provided to the integrated circuit 20 via test port 27 and is stored in the volatile memory circuit 24. Goodman teaches that during the test mode, the secure electronic keys are inaccessible (see Goodman, col. 7, lines 53-55, col. 8, lines 48-52).

However, Goodman teaches using the private test key in the test mode, but does not teach or suggest using the private test key in the *work* mode. Likewise, Goodman teaches using the secure electronic key in the work mode, but does not teach or suggest using the secure electronic key in the *test* mode. Thus, Goodman teaches using separate keys in separate respective modes. Nowhere does Goodman teach using a single key in multiple modes. Specifically, Goodman does not teach that the encryption processor 23 (or 33, 43, 66) using a private test key (or a secure electronic key) in a first mode for encryption operations and for test operations and in a second mode in which the private test key (or the secure electronic key) is only used for timestamping operations. Therefore, Fischer in light of Goodman does not teach all of the claim features.

The only teaching of providing a processor that uses a single key in multiple modes for test, encryption, and timestamping operations is found in Applicant’s disclosure. Based on the teachings of Fischer and Goodman, assuming, *arguendo*, that there is motivation to combine these references, one of ordinary skill in the art would not modify the references as alleged by the Action. One of ordinary skill in the art might modify the processor module 6 of Fischer to have two modes and use

the secret private key of Fischer in the work mode, similar to that of Goodman, and add a test mode to the processor module 6 of Fischer to use the private test key in the test mode, similar to that of Goodman. Thus, assuming that proper motivation to combine could be found, the combined teachings might suggest using separate keys in separate modes. However, this modification does not teach or suggest providing a processor that uses a single key in different operations in different modes. The Action impermissibly relies on Applicant's own disclosure to bridge this gap between the teachings of Fischer in view of Goodman and the claimed invention. Without Applicant's teachings of providing a processor that uses a single key in multiple modes for different operations, one of ordinary skill in the art would not modify the combined teachings of Fischer and Goodman as stated in the Action to render claim 1 obvious. Additionally, Menezes does not teach an encryption processor using a single key in multiple modes to supplement Fischer and Goodman. Thus, the combined teachings of Fischer, Goodman, and Menezes do not teach or suggest the features of claim 1, in contrast with the statements of the Action.

Applicant notes that a further description of Fischer, Goodman, and Menezes was included with the previous Amendment filed June 24, 2005 and the Request for Reconsideration filed October 28, 2005. Applicant respectfully requests that the Examiner also reconsider the arguments presented in the previous filings, which are not included herein, for brevity. Thus, for at least the reasons stated above, the combined teachings of Fischer, Goodman, and Menezes do not teach or suggest all of the features recited in claim 1. Therefore, the Action does not establish a *prima facie* case of obviousness to reject claim 1 under 35 U.S.C. § 103(a) based on the combined teachings of Goodman, Fischer, and Menezes.

Accordingly, claim 1 is allowable over the cited references and allowance thereof is respectfully requested. Claims 2-6 and 8-10, which depend from claim 1, are also in condition for allowance because of their dependence on an allowable claim.

(B) Claim 11 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 12-14, which depend from claim 11, are also in condition for allowance because of their dependence on an allowable claim.

(C) Claim 15 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 16-18, which depend from claim 15, are also in condition for allowance because of their dependence on an allowable claim.

(D) Claim 20 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 21-24, which depend from claim 20, are also in condition for allowance because of their dependence on an allowable claim.

(E) Claim 25 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested.

Accordingly, claims 1-6, 8-18, and 20-25 are in condition for allowance and allowance thereof is respectfully requested.

**Conclusion**

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

Dated:

Respectfully submitted,

Nov. 28, 2005

Edward W. Yee  
Edward W. Yee  
Reg. No.: 47,294  
Attorney For Applicant  
VENABLE LLP  
P.O. Box 34385  
Washington, DC 20043-9998  
(202) 344-4000  
(202) 344-8300 (Fax)